Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/KR04/003212

International filing date: 08 December 2004 (08.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: KR
Number: 10-2003-0088895
Filing date: 09 December 2003 (09.12.2003)

Date of receipt at the International Bureau: 02 February 2005 (02.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 특허출원 2003년 제 0088895 호
Application Number 10-2003-0088895

출 원 년 월 일 : 2003년 12월 09일
Date of Application DEC 09, 2003

출 원 인 : 삼성전자주식회사 외 5명
Applicant(s) SAMSUNG ELECTRONICS CO., LTD., et al.

2004 년 12 월 27 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【제출일자】 2003.12.09

【발명의 명칭】 ＩＥＥＥ 802.16 무선 ＭＡＮ 시스템에서 서비스별 트래픽 암호화 키 생성 및 분배 방법

【발명의 영문명칭】 A Method for Generating and Distributing Traffic Encryption Key for Each Service Type in the IEEE 802.16 WirelessMAN System

【출원인】

【명칭】 한국전자통신연구원

【출원인코드】 3-1998-007763-8

【대리인】

【명칭】 유미특허법인

【대리인코드】 9-2001-100003-6

【지정된변리사】 이원일

【포괄위임등록번호】 2001-038431-4

【발명자】

【성명의 국문표기】 조석헌

【성명의 영문표기】 CHO,SEOK HEON

【주민등록번호】 770127-1543416

【우편번호】 570-976

【주소】 전라북도 익산시 신동 775-21번지

【국적】 KR

【발명자】

【성명의 국문표기】 박애순

【성명의 영문표기】 PARK,AE SOON

【주민등록번호】 640920-2401130

【우편번호】 305-755

【주소】 대전광역시 유성구 어은동 한빛아파트 138동 301호

【국적】 KR

【발명자】

【성명의 국문표기】 윤철식

【성명의 영문표기】 YOON,CHUL SIK

【주민등록번호】 641220-1009115

【우편번호】 139-777

【주소】 서울특별시 노원구 하계동 선경아파트 4동 402호

【국적】 KR

【발명자】

【성명의 국문표기】 김경수

【성명의 영문표기】 KIM,KYUNG SOO

【주민등록번호】 570129-1403316

【우편번호】 305-707

【주소】 대전광역시 유성구 신성동 한울아파트 109동 1702호

【국적】 KR

【발명자】

【성명의 국문표기】 안지환

【성명의 영문표기】 AHN,JEE HWAN

【주민등록번호】 560617-1460611

【우편번호】 305-804

【주소】 대전광역시 유성구 신성동 149-7번지

【국적】 KR

【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다.
대리인 유미특
허법인 (인)

【수수료】

【기본출원료】 13 면 29,000 원

【가산출원료】 0 면 0 원

【우선권주장료】 0 건 0 원

【심사청구료】 0 항 0 원

【합계】 29,000 원

【감면사유】 정부출연연구기관

【감면후 수수료】 14,500 원

【기술이전】

【기술양도】 희망

【실시권 허여】 희망

【기술지도】 희망

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 IEEE 802.16 무선 MAN(Metropolitan Area Network) 시스템에서 서비스별 트래픽 암호화 키 생성 및 분배 방법에 관한 것이다.

본 발명에 따르면, 유니캐스트, 멀티캐스트, 브로드캐스트를 포함하는 서비스 중 어느 하나 이상의 서비스에 대하여 각 서비스 별로 트래픽 암호화 키를 생성 및 분배한다. 이때, 단말은 키 요청 메시지를 이용하여 서비스 별 트래픽 암호화 키 할당을 요구한다. 상기 키 요청 메시지에 서비스 타입이 포함되며, 단말이 제공받고자 하는 서비스 유형이 멀티캐스트 서비스인 경우, 상기 키 요청 메시지에 멀티 캐스트 그룹 ID가 포함된다. 그리고, 단말이 요구한 서비스 별 트래픽 암호화 키 할당이 실패할 때, 키 거절 메시지의 에러 코드를 이용하여 실패 이유를 나타낸다.

이와 같이, 본 발명에 따르면 유니캐스트 서비스 뿐만 아니라 멀티캐스트 서비스와 브로드캐스트 서비스용 암호화키를 생성하고 분배할 수 있기 때문에, 다양한 서비스에 대하여 있어서 보다 안정성 있는 서비스를 제공할 수 있다.

【대표도】

도 2

【색인어】

IEEE 802.16 무선 MAN, 서비스, 트래픽 암호화 키, 데이터 보안, 멀티캐스트, 브로드캐스트

【명세서】

【발명의 명칭】

Ｉ ＥＥＥ 802.16 무선 ＭＡＮ 시스템에서 서비스별 트래픽 암호화 키 생성 및 분배 방법{A Method for Generating and Distributing Traffic Encryption Key for Each Service Type in the IEEE 802.16 WirelessMAN System}

【도면의 간단한 설명】

도 1은 본 발명의 실시예에 따른 서비스 별 키 생성 및 분배 절차도를 나타내는 도면이다.

도 2는 본 발명의 실시예에 따른 트래픽 암호화 키 할당 요구 메시지에서 추가되는 파라미터 테이블을 나타내는 도면이다.

도 3 및 도 4는 도 2에 도시된 파라미터들의 내용을 포함한 테이블을 나타내는 도면이다.

도 5는 본 발명의 실시예에 따른 트래픽 암호화 키 할당 요구 거절 메시지에서 추가 사항 테이블을 나타내는 도면이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<5> 본 발명은 트래픽 암호화 키 생성 및 분배 방법에 관한 것으로서, 특히 IEEE 802.16 무선 MAN(Metropolitan Area Network) 시스템에서 서비스별 트래픽 암호화 키 생성 및 분배 방법에 관한 것이다.

<6> IEEE 802.16 무선(Wireless) MAN(Metropolitan Area Network) 기반의 무선 인터넷 시스템에서는 안정성 있는 서비스를 제공하기 위해 트래픽 데이터에 대한 암호화 기능을 정의하고 있다. 트래픽 데이터에 대한 암호화 기능은 서비스의 안정성 및 망의 안정성을 위해 필요한 요구사항으로 대두되고 있고, 정당한 서비스를 제공하기 위한 기본 조건이다.

<7> 기존 IEEE 802.16 무선 MAN 시스템에서는 트래픽 데이터를 암호화하기 위해 트래픽 연결 설정 절차에 앞서서 해당 트래픽 연결에 사용될 트래픽 암호화 키를 생성하고 분배하는 방식을 정의하고 있다.

<8> 구체적으로, 단말과 기지국은 암호화 키의 생성 및 분배를 위해, 인증 관련 메시지인 PKM-REQ 메시지와 PKM-RSP 메시지를 사용한다. 즉, 단말은 PKM-REQ 메시지 중 하나의 내부 메시지인 키 요청(Key Request) 메시지를 기지국으로 전송함으로써 트래픽 암호화 키 할당을 요구하고, 기지국은 이에 대한 응답을 단말로 보낸다. 구체적으로 기지국은 트래픽 암호화 키 할당이 성공하였을 경우에는 키 응답(Key Reply) 메시지를 단말로 송부하고, 실패하였을 경우에는 키 거절(Key Reject) 메시지를 단말로 전송한다. 이와 같은 트래픽 암호화 키 할당 절차를 통해 할당받은 트래픽 암호화 키를 이용하여 단말과 기지국은 모든 트래픽 데이터를 암호화하여 전송한다.

<9> 이와 같은 기존의 IEEE 802.16 무선 MAN 시스템에서 정의하는 트래픽 암호화 키 생성 및 분배 방식은 단말과 기지국 사이의 유니 캐스트(unicast) 서비스에만 국한된 방식이라는 단점이 있다.

<10> 한편, IEEE 802.16 무선 MAN 시스템이 더욱 더 많은 가입자에게 확장성 있는 서비스를 제공하고 다양한 서비스를 안정적으로 제공하기 위해서는 유니캐스트 서비스

뿐만 아니라 멀티캐스트(Multicast) 서비스와 브로드 캐스트(Broadcast) 서비스까지도 고려해야 할 필요가 있다.

<11> 그러나, IEEE 802.16 무선 MAN 시스템에서 멀티캐스트 서비스를 제공할 경우 서비스 암호화를 위하여 고려하여야 할 사항들이 존재한다. 즉, 해당 멀티 캐스트 서비스에 가입하지 않은 동일 시스템의 사용자들에 대한 서비스를 제한하거나, 브로드 캐스트 서비스를 제공할 경우 타 사업자의 가입자들에 대한 서비스를 제한하는 방안이 고려되어야 하는데, 이와 같은 서비스의 제한은 현재의 규격으로는 구체적인 정의가 되어 있지 않다.

【발명이 이루고자 하는 기술적 과제】

<12> 본 발명이 이루고자 하는 기술적 과제는 상기한 종래 기술의 문제점을 해결하기 위한 것으로서, 본 발명은 IEEE 802.16 무선 MAN 시스템에서 기존에 정의하였던 트래픽 암호화 키 생성 및 분배 방식을 확장하고 보완하여 시스템에서 제공할 수 있는 다양한 서비스 별 트래픽의 암호화를 위한 키 생성 및 분배 방안을 제안하기 위한 것이다.

<13> 또한, 본 발명은 트래픽 암호화 키 생성 절차에 있어서 실패가 발생하였을 경우 수용할 수 있는 처리 방안을 제시하기 위한 것이다.

<14> 또한, 본 발명은 기존에 정의되어 있는 키 생성 및 분배 메시지에 서비스 타입을 고려하여 키 생성이 가능하도록 관련 파라미터를 추가하고, 이를 정의함으로써 합법적인 가입자에게 합법적인 서비스를 제공하여 망의 안정성 및 서비스 효율성을 높이기 위한 것이다.

【발명의 구성 및 작용】

<15> 이와 같은 목적을 달성하기 위한 본 발명의 특징에 따른 트래픽 암호화 키 생성 및 분배 방법은 IEEE 802.16 무선 MAN 기반의 무선 인터넷 시스템에서 트래픽 암호화 키를 생성 및 분배하는 방법으로서,

<16> 유니캐스트, 멀티캐스트, 브로드캐스트를 포함하는 서비스 중 어느 하나 이상의 서비스에 대하여 각 서비스 별로 트래픽 암호화 키를 생성 및 분배하는 것을 특징으로 한다.

<17> 여기서, 단말은 키 요청 메시지를 이용하여 서비스 별 트래픽 암호화 키 할당을 요구하는 것을 특징으로 한다.

<18> 이때, 상기 키 요청 메시지에 서비스 타입이 포함되는 것이 바람직하다. 또한, 상기 단말이 제공받고자 하는 서비스 유형이 멀티캐스트 서비스인 경우, 상기 키 요청 메시지에 멀티 캐스트 그룹 ID가 포함되는 것이 바람직하다.

<19> 그리고, 단말이 요구한 서비스 별 트래픽 암호화 키 할당이 실패할 때, 키 거절 메시지의 에러 코드를 이용하여 실패 이유를 나타내는 것을 특징으로 한다.

<20> 이때, 단말이 제공받고자 요구하였던 서비스 유형이 제공 불가능한 경우, 상기 에러 코드에 지원하지 않는 서비스 타입(Unsupported Service Type)을 기재하는 것을 특징으로 한다. 그리고, 단말이 제공받고자 요구하였던 멀티캐스트 서비스 종류의 서비스가 제공 불가능한 경우, 상기 에러 코드에 권한없는 멀티캐스트 서비스 그룹 ID(Unauthorized Multicast Service Group ID)를 기재하는 것을 특징으로 한다.

<21> 이하에서는 도면을 참조하여 본 발명의 실시예를 상세히 설명한다.

<22> 도 1은 본 발명의 실시예에 따른 서비스 별 트래픽 암호화 키 생성 및 분배 절차도이다.

<23> 단말(SS, 101)과 기지국 (BS, 102) 사이의 초기화 절차(S100)가 끝나면, 단말은 본격적으로 트래픽 서비스를 제공받을 수 있게 된다. 그리고, 이와 같이 제공받는 트래픽 데이터에 대한 암호화를 하기 위해 서비스 별 트래픽 암호화 키 생성 및 분배 절차를 거치게 된다 (S110).

<24> 이하에서는 본 발명의 실시예에 따른 서비스별 트래픽 암호화 키 생성 및 분배 절차(S110)를 보다 상세히 설명한다.

<25> 먼저, 단말(101)은 자신이 원하는 서비스 종류에 대한 트래픽 암호화 키를 할당받기 위해 기지국으로 PKM-REQ 메시지인 키 요청(Key Request) 메시지를 송신한다 (S111). 이 메시지를 수신한 기지국은 수신된 메시지의 모든 필드 값들을 바탕으로 하여 트래픽 암호화 키 생성 메커니즘으로 해당 단말에 트래픽 암호화키를 할당한다. 구체적으로, 기지국(102)은 트래픽 암호화 키 생성이 성공하면, PKM-RSP 메시지인 키 응답(Key Reply) 메시지를 단말로 전송하고, 실패하면 키 거절(Key Reject) 메시지를 단말로 전송한다. 이와 같이, 기지국이 키 응답 또는 키 거절 메시지를 단말에 전송함으로써, 단말에 대한 트래픽 암호화 키 생성 및 분배 절차가 끝나게 된다 (S112).

<26> 이때, 기지국(102)이 단말로 전송하는 키 응답 메시지에는 단말이 요구하는 서비스 종류에 따른 트래픽 암호화 키가 포함되어 있으며, 이를 수신한 단말(101)은 해당 서비스를 제공받을 때 기지국으로부터 수신한 트래픽 암호화 키를 이용하여 트래

픽 데이터에 대하여 암호화하거나 복호화를 수행한다. 이와달리, 키 거절 메시지에는 기지국이 트래픽 암호화 키를 할당하는데 있어 실패한 이유가 포함되어 있다.

<27> 도 2는 기존의 키 요청 메시지에 본 발명의 실시예에 따른 서비스 별 트래픽 키 생성 및 분배 방법으로 인해 추가되는 파라미터들의 테이블을 나타내는 도면이다.

<28> 도 2에서, 서비스 타입(Service Type)(201)은 단말이 어떠한 유형의 서비스를 제공받고자 하는지를 나타낸다. 기지국은 이 서비스 타입의 값을 보고 해당 서비스 유형에 맞게 트래픽 암호화 키를 할당하는 것이다.

<29> 멀티캐스트 서비스 그룹(Multicast Service Group) ID (202)는 단말이 트래픽 암호화 키를 할당받고자 하는 서비스 유형이 멀티캐스트 서비스일 때만 존재하는 것으로서, 멀티캐스트 서비스 그룹의 식별자 역할을 한다. 이 멀티캐스트 서비스 그룹 ID는 단말이 멀티캐스트 서비스를 제공받더라도 가입하지 않은 타 멀티캐스트 서비스 그룹의 서비스에 제한을 두기 위한 목적으로도 사용된다.

<30> 도 3은 도 2에 도시한 서비스 타입 필드의 속성 (300)을 나타내는 도면이다.

<31> 도 3에 도시한 서비스 타입 필드의 값은 이 필드로 할당받으려는 트래픽 암호화 키의 해당 서비스 종류를 나타낸다. 예를 들면, 필드 값이 "0"이면 유니캐스트 서비스에 해당하는 트래픽 암호화 키 할당을 요구하는 것이고, "1"이면 멀티캐스트 서비스에 해당하는 트래픽 암호화 키 할당을 요구하는 것이다.

<32> 도 4는 도 2에 도시된 멀티캐스트 서비스 그룹 ID 필드의 속성(400)을 나타내는 도면이다. 멀티캐스트 서비스 그룹 ID는 IEEE 802.16 무선 MAN 시스템에서 제공하는 멀티캐스트 서비스 그룹의 식별자이다.

<33> 도 5는 도 1에 도시된 트래픽 암호화 키 할당 실패 시 기지국에서 단말로 전송하는 키 거절 메시지에 포함되는 에러코드로서, 기존의 IEEE 802.16에서 정의한 에러코드에서 본 발명의 제안에 따라 추가된 사항을 나타낸 테이블이다.

<34> 도 5를 참조하면, 서비스별 트래픽 암호화 키를 할당받기 위해 단말은 키 요청 메시지에 서비스 타입으로 서비스 종류를 정의하는데, 만약 이 값이 지원 불가능한 값이면 기지국은 "지원하지 않는 서비스 타입(Unsupported Service Type)"값 (501)을 가지는 에러코드를 포함한 키 거절 메시지를 단말로 송신한다. 또한, 단말이 전송한 키 요청 메시지의 멀티캐스트 서비스 그룹 ID를 가진 멀티캐스트 서비스에 대한 트래픽 암호화키를 할당할 수 없을 경우에는 기지국은 "권한이 없는 멀티캐스트 서비스 그룹 ID(Unauthorized Multicast Service Group ID)"값(502)을 가지는 에러 코드를 포함한 키 요청 메시지를 단말로 응답한다.

<35> 이상에서 설명한 바와 같이, 본 발명의 실시예에 따르면, 다음과 같은 효과가 있다.

<36> 첫째, 시스템에서 제공하는 다양한 서비스별 트래픽 암호화 키를 할당할 수 있는 기능이 지원가능하게 되고, 그 결과 멀티캐스트 서비스나 브로드캐스트 서비스와 같은 다양한 서비스를 안정적으로 제공할 수 있기 때문에 많은 가입자를 유도해 서비스의 활성화를 도모할 수 있다.

<37> 둘째, 서비스 별로 트래픽 암호화 키를 생성하고 관리함으로써 서비스의 더욱 강력한 보안을 유지할 수 있다.

<38> 셋째, 멀티캐스트 서비스의 경우 멀티캐스트 서비스 그룹별로 할당된 그룹 트래픽 암호화 키가 다르므로 그룹별로 보안유지가 가능하다.

<39> 이상에서는 본 발명의 실시예에 대하여 설명하였으나, 본 발명은 상기한 실시예에만 한정되는 것은 아니고, 그 외의 다양한 변경이나 변형이 물론 가능하다.

【발명의 효과】

<40> 이상에서 설명한 바와 같이, 본 발명에 따르면 유니캐스트 서비스를 비롯하여 멀티캐스트 서비스와 브로드캐스트 서비스 용 암호화키를 생성하고 분배할 수 있기 때문에, 다양한 서비스에 대하여 보다 확장적이고 안정성있는 서비스를 제공할 수 있다.

【특허청구범위】

【청구항 1】

IEEE 802.16 무선 MAN 기반의 무선 인터넷 시스템에서 트래픽 암호화 키를 생성 및 분배하는 방법에 있어서,

유니캐스트, 멀티캐스트, 브로드캐스트를 포함하는 서비스 중 어느 하나 이상의 서비스에 대하여 각 서비스 별로 트래픽 암호화 키를 생성 및 분배하는 것을 특징으로 하는 트래픽 암호화 키 생성 및 분배 방법.

【청구항 2】

제1항에 있어서,

단말이 키 요청 메시지를 이용하여 서비스 별 트래픽 암호화 키 할당을 요구하는 것을 특징으로 하는 트래픽 암호화 키 생성 및 분배 방법.

【청구항 3】

제2항에 있어서, 상기 키 요청 메시지에 서비스 타입이 포함되는 것을 특징으로 하는 트래픽 암호화 키 생성 및 분배 방법.

【청구항 4】

제3항에 있어서,

상기 단말이 제공받고자 하는 서비스 유형이 멀티캐스트 서비스인 경우, 상기 키 요청 메시지에 멀티 캐스트 그룹 ID가 포함되는 것을 특징으로 하는 트래픽 암호화 키 생성 및 분배 방법.

【청구항 5】

제1항에 있어서,

단말이 요구한 서비스 별 트래픽 암호화 키 할당이 실패할 때, 키 거절 메시지의 에러 코드를 이용하여 실패 이유를 나타내는 것을 특징으로 하는 트래픽 암호화 키 생성 및 분배 방법.

【청구항 6】

제5항에 있어서,

단말이 제공받고자 요구하였던 서비스 유형이 제공 불가능한 경우, 상기 에러 코드에 지원하지 않는 서비스 타입(Unsupported Service Type)을 기재하는 것을 특징으로 하는 트래픽 암호화 키 생성 및 분배 방법.

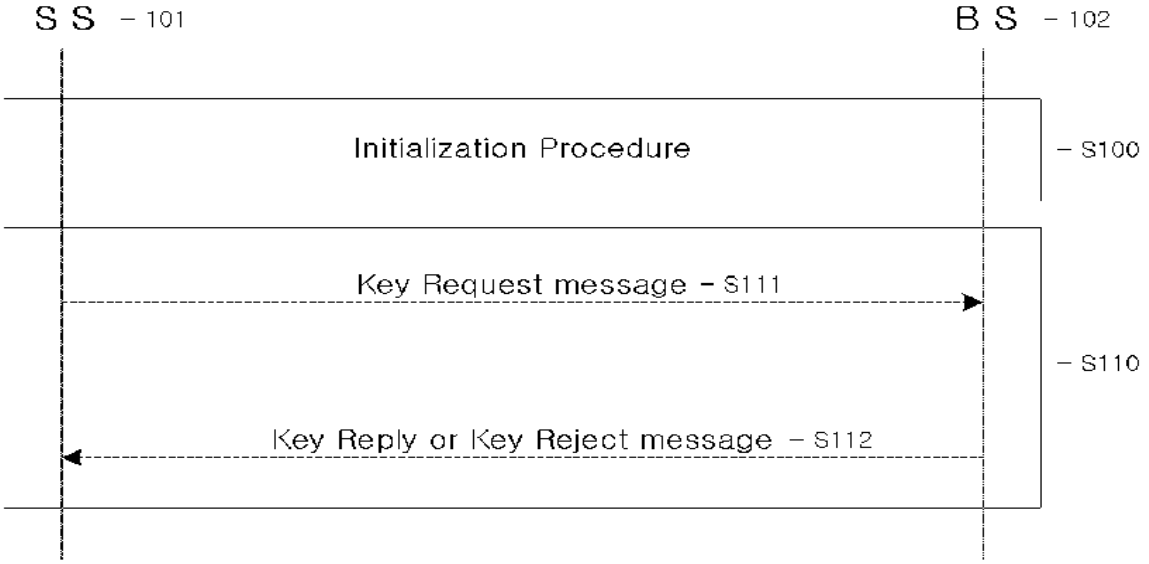
【청구항 7】

제5항에 있어서,

단말이 제공받고자 요구하였던 멀티캐스트 서비스 종류의 서비스가 제공 불가능한 경우, 상기 에러 코드에 권한없는 멀티캐스트 서비스 그룹 ID(Unauthorized Multicast Service Group ID)를 기재하는 것을 특징으로 하는 트래픽 암호화 키 생성 및 분배 방법.

【도면】

【도 1】



【도 2】

PKM-REQ (Key Request) attributes – 200

	Attribute	Contents
201 -	Service Type	Service Type (Unicast or multicast or broadcast)
202 -	Multicast Service Group ID	Identifier of multicast service group

【도 3】

Service Type attributes - 300

Type	Length	Value
28	1	0: Unicast Service 1: Multicast Service 2 : Broadcast Service 3-255: reserved.

【도 4】

Multicast Service Group ID attributes - 400

Type	Length	Value
29	1	Identifier of the multicast service group

【도 5】

Error-code attribute code values – 500

	Error Code	Messages	Contents
501 -	7	Key Reject	Unsupported Service Type
502 -	8	Key Reject	Unauthorized Multicast Service Group ID